

REMARKS

Claims 1-3, 5, 9-13, 18, 21-23 and 25-27 are pending. By this Amendment, the Specification at paragraph [0049] is amended. No new matter is added.

The Specification at paragraph [0049] is amended to address the claim rejection under 35 U.S.C. §101 applied in the Office Action.

For the following reasons, reconsideration is respectfully requested.

Claim Rejection Under 35 U.S.C. § 101

Claims 1, 10, 22 and 25 are rejected under 35 U.S.C. § 101. The rejection is respectfully traversed.

During a June 2, 2009 personal interview, Examiner Brown stated that paragraph [0049] of the Specification discloses software processing, which pertains to the rejection of claims 1, 10 and 22 under U.S.C. § 101. Accordingly, paragraph [0049] of the Specification is amended to delete reference to the software processing.

Additionally, claims 25-27 are stated as reciting subject matter that is not patentable. Applicants respectfully disagree because claims 25-27 recite a method being processed in an encryption apparatus, and the recited start key signal of claim 25 and the recited data key valid signal of claim 26, for example, have structural and functional interrelationship with the recited encryption apparatus. Accordingly, claims 25-27 recite patentable subject matter.

Accordingly, withdrawal of this rejection is respectfully requested.

Claim Rejections Under 35 U.S.C. § 103(a)

Claims 1, 2, 5, 9-11, 18 and 21-23 are rejected under 35 U.S.C. § 103(a) over Wasilewski (U.S. Patent No. 5,420,866), in view of Daemen ("AES Proposal: Rijndael," March 1999). The rejection is respectfully traversed.

It is respectfully submitted that Wasilewski and Daemen, either individually or in combination, fail to disclose or suggest an apparatus for encrypting/decrypting a real-time input stream comprising a control unit that generates a start key signal when a new round key is needed, and a key schedule unit that provides a round key for every round in accordance with the start key signal and an input key having a variable size to provide the round key for the encryption or decryption for each round, as recited in claim 1.

Also, Wasilewski and Daemen, either individually or in combination, fail to disclose or suggest each and every feature of claims 10 and 22 that recite similar features of varying scope.

Specifically, it is acknowledged in the Office Action that Wasilewski is deficient, but Daemen is applied as remedying the deficiencies of Wasilewski. However, Daemen fails to remedy the deficiencies of Wasilewski because Daemen simply discloses that round keys are derived from a cipher key by means of a key schedule (see 4.2.4 and 4.3 of Daemen). That is, Daemen discloses a cipher key that is used to derive the round keys according to a schedule.

First, the cipher key of Daemen does not show a start key signal. In other words, the cipher key of Daemen is simply an original source key for deriving round keys. The cipher key of Daemen is not a control signal like the recited start key signal (see 4.1 and FIG. 1; and 4.2.4 and FIG. 5 of Daemen).

Second, since the cipher key is used to derive the round keys according to a schedule,

Daemen fails to disclose whether the cipher key is generated for every round when a new round key is needed in accordance with the start key. Rather, since one cipher key is used, and since the one cipher key is used to derive the round keys according to a schedule, Daemen discloses that all round keys for block encryption are derived and selected from the cipher key at one time (see 4.3 and 4.3.2 of Daemen).

Accordingly, Daemen fails to disclose the features lacking in Wasilewski so that Wasilewski and Daemen, either individually or in combination, fail to disclose each and every feature of claim 1. Wasilewski and Daemen, either individually or in combination, fail to disclose each and every feature of claims 10 and 22 for similar reasons.

Thus, claims 1, 10 and 22 are patentably distinguishable over the applied references and their combination. Claims 2, 5 and 9, which depend from claim 1; claims 11, 18 and 21, which depend from claim 10; and claim 23, which depend from claim 22, are likewise patentably distinguishable over the applied references and their combination for at least the reasons discussed above and/or for the additional features they recite. Withdrawal of the rejection is respectfully requested.

Claims 3, 12 and 13 are rejected under 35 U.S.C. § 103(a) over Wasilewski, in view of Daemen, and further in view of Mroczkowski ("Implementation of the block cipher Rijndael using Altera FPGA," May 2000). The rejection is respectfully traversed.

As discussed above, Wasilewski and Daemen, either individually or in combination, fail to disclose or suggest each and every feature of claim 1, from which claim 3 depends, and fail to disclose or suggest each and every feature of claim 10, from which claims 12 and 13 depend. As

Mroczkowski fails to remedy at least the noted deficiencies of Wasilewski and Daemen, either individually or in combination, claims 3, 12 and 13 are patentably distinguishable over the applied references and their combination for at least the reasons stated above and/or their added features. Withdrawal of the rejection is respectfully requested.

Claims 25-27 are rejected under 35 U.S.C. § 103(a) over Wasilewski, in view of Daemen, and further in view Vanstone (U.S. Patent No. 6,212,281). The rejection is respectfully traversed.

It is respectfully submitted that Wasilewski, Daemen, and Vanstone, either individually or in combination, fail to disclose or suggest, a method of controlling a data protection key, the method being processed in a encryption apparatus comprising generating a start key signal when a generation of a new data key is needed in the encryption apparatus, as recited in claim 25.

As discussed above, Wasilewski and Daemen, either individually or in combination, fail to disclose or suggest the recited feature regarding the generating of a start key signal when a generation of a new data key is needed. Vanstone fails to remedy at least this noted deficiency of Wasilewski and Daemen. Accordingly, Wasilewski, Daemen and Vanstone, either individually or in combination, fail to disclose or suggest each and every feature of claim 25. Thus, claim 25 is patentably distinguishable over the applied references and their combination. Claims 26 and 27, which depend from claim 25, are likewise patentably distinguishable over the applied references and their combination for at least the reasons discussed above and/or for the additional features they recite. Withdrawal of the rejection is respectfully requested.

Conclusion

In view of the above amendment and/or remarks, applicant believes the pending application is in condition for allowance.

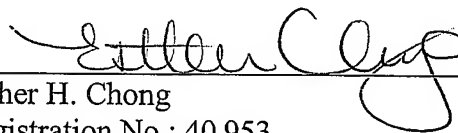
Should there be any outstanding matters that need to be resolved in the present application, the Examiner is respectfully requested to contact Seth S. Kim, Reg. No. 54,577, at the telephone number of the undersigned below, to conduct an interview in an effort to expedite prosecution in connection with the present application.

If necessary, the Commissioner is hereby authorized in this, concurrent, and future replies to charge payment or credit any overpayment to Deposit Account No. 02-2448 for any additional fees required under 37.C.F.R. §§1.16 or 1.17; particularly, extension of time fees.

Dated: **AUG 25 2009**

Respectfully submitted,

By



Esther H. Chong

Registration No.: 40,953

BIRCH, STEWART, KOLASCH & BIRCH, LLP

8110 Gatehouse Road

Suite 100 East

P.O. Box 747

Falls Church, Virginia 22040-0747

(703) 205-8000

Attorney for Applicant